



UNITED STATES PATENT AND TRADEMARK OFFICE

mm
UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/699,005	10/30/2003	Michael Scheidell	1012-003U	1429

29973 7590 04/10/2007
CAREY, RODRIGUEZ, GREENBERG & PAUL LLP
ATTN: STEVEN M. GREENBERG, ESQ.
950 PENINSULA CORPORATE CIRCLE
SUITE 3020
BOCA RATON, FL 33487

EXAMINER

SHERKAT, AREZOO

ART UNIT	PAPER NUMBER
----------	--------------

2131

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

10/699,005

Applicant(s)

SCHEIDELL, MICHAEL

Examiner

Arezoo Sherkat

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 October 2003.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>10/30/03, 9/13/04, 4/29/05</u> | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Claims 1-20 are presented for examination.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-5 are rejected under 35 U.S.C. 102(e) as being anticipated by Currie et al., (U.S. Publication No. 2003/0188194 and Currie hereinafter).

Regarding claim 1, Currie discloses a computer network intrusion detection system comprising: an intrusion detector for detecting external attacks upon a computer network, an analyzer coupled to said intrusion detector for analyzing each detected attack and determining a characteristic indicative thereof (i.e., scan engine)(par. 43); and a filter coupled to said analyzer for generating an alert based upon characteristics of a plurality of attacks (i.e., alert engine)(par. 44-45).

Regarding claim 2, Currie discloses the system according to claim 1 wherein said filter generates a first alert signal in response to an attack having a new characteristic,

Art Unit: 2131

and further generates a second alert signal indicative of a predetermined plurality of attacks having the new characteristic occurring within a predetermined time (i.e., displaying the status rates on the scale of "low", "medium", and "high" ... within a predetermined time period)(par. 44-45 and 86).

Regarding claim 3, Currie discloses the system according to claim 1 wherein said filter generates a first alert signal in response to an attack having a new characteristic, and further generates a subsequent first alert signal in response to a subsequent attack having the new characteristic occurring after an absence of attacks having the new characteristic occurring within a predetermined time (par. 44-45 and 86).

Regarding claim 4, Currie disclose the system according to claim 1 wherein said filter generates the alert in response to attacks of a predetermined characteristic exceeding a predetermined rate or frequency (i.e., displaying numeric ratings of frequency of vulnerabilities)(par. 86).

Regarding claim 5, Currie discloses the system according to claim 4 wherein the predetermined rate or frequency deterministically varies (par. 86).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2131

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 6-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Currie et al., (U.S. Publication No. 2003/0188194 and Currie hereinafter), in view of Hrabik et al., (U.S. Publication No. 2002/0178383 and Hrabik hereinafter).

Regarding claim 6, Currie discloses detecting vulnerabilities of different websites on the Internet (par. 5-6).

Currie does not expressly disclose handling intrusion detection with respect to multiple networks.

However, Hrabik discloses an intrusion detector for detecting attacks upon a second computer network (i.e., a plurality of networks), wherein said filter is further coupled to said second intrusion detector and communicates the alert to the computer network in response to attacks of a predetermined characteristic upon the second computer network exceeding a predetermined rate or frequency (par. 59-61).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Currie with teachings of Hrabik because it would allow to include an intrusion detector for detecting attacks upon a second computer network as disclosed by Hrabik. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Hrabik to protect a target network from both internal and external intruders (Hrabik, par. 11).

Art Unit: 2131

suggestion of Hrabik to protect a target network from both internal and external intruders (Hrabik, par. 11).

Regarding claim 7, Currie discloses detecting vulnerabilities of different websites on the Internet (par. 5-6).

Currie does not expressly disclose handling intrusion detection with respect to multiple networks.

However, Hrabik discloses further comprising: a vulnerability tester coupled to said analyzer for testing a second computer network for a vulnerability to an attack characteristic detected by said analyze (par. 59-61).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Currie with teachings of Hrabik because it would allow to include an intrusion detector for detecting attacks upon a second computer network as disclosed by Hrabik. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Hrabik to protect a target network from both internal and external intruders (Hrabik, par. 11).

Regarding claim 8, Currie discloses detecting vulnerabilities of different websites on the Internet (par. 5-6).

Currie does not expressly disclose handling intrusion detection with respect to multiple networks.

However, Hrabik discloses further comprising: an second intrusion detector for detecting external attacks upon a second computer network; a second analyzer coupled to said second intrusion detector for analyzing each detected attack upon the second network and determining a characteristic indicative thereof, wherein said filter is further coupled to said second analyzer and further compares the attack characteristics determined by said analyzer and said second analyzer and generates a general attack alert in response to a substantial similarity in the comparison (par. 59-61).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Currie with teachings of Hrabik because it would allow to include an intrusion detector for detecting attacks upon a second computer network as disclosed by Hrabik. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Hrabik to protect a target network from both internal and external intruders (Hrabik, par. 11).

Regarding claim 9, Currie discloses detecting vulnerabilities of different websites on the Internet (par. 5-6).

Currie does not expressly disclose handling intrusion detection with respect to multiple networks.

However, Hrabik discloses further comprising: a second intrusion detector for detecting external attacks upon a second computer network; a second analyzer coupled to said second intrusion detector for analyzing each detected attack upon the

second network and determining a characteristic indicative thereof, wherein said filter is further coupled to said second analyzer and further compares the attack characteristics determined by said analyzer and said second analyzer and generates a specific attack alert in response to a substantial absence of similarity in the comparison (i.e., an analyzer might determine that a particular events warrants additional scrutiny because a network device on which it was detected is particularly vulnerable to the type of attacks this event is associated with)(par. 59-61).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Currie with teachings of Hrabik because it would allow to include an intrusion detector for detecting attacks upon a second computer network as disclosed by Hrabik. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Hrabik to protect a target network from both internal and external intruders (Hrabik, par. 11).

Regarding claim 10, Hrabik discloses the system according to claim 9 further comprising an alert generator for generating an alert indicative of the specific attack on the one of the networks experiencing the attacks having the absence of similarity of attacks on the other of the networks (i.e., an analyzer might determine that a particular event warrants additional scrutiny because a network device on which it was detected is particularly vulnerable to the type of attacks this event is associated with)(par. 59-61).

Regarding claim 11, Hrabik discloses the system according to claim 9 further comprising: a vulnerability tester coupled to said filter for testing the one of the networks not experiencing the attacks for a vulnerability to the attack characteristic experienced by the other of the computer networks (par. 59).

Regarding claim 12, Currie discloses the security verification system can maintain and provide security scores and corresponding graphical indicators of individual security attributes, both current and/or historical, of one or more on-line services (par. 23).

Moreover, Hrabik discloses a method of generating a network intrusion alert for a first network coupled to a multiple client network system comprising the steps of:

determining a characteristic of an attack upon the first network, determining if the characteristic matches a characteristic of an attack upon a second client coupled to the multiple client network system, and generating a first alert in response to an absence of the match (par. 59-61).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Currie with teachings of Hrabik because it would allow to include an intrusion detector for detecting attacks upon a second computer network as disclosed by Hrabik. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Hrabik to protect a target network from both internal and external intruders (Hrabik, par. 11).

Regarding claim 13, Currie discloses the method according to claim 12 further comprising the step of generating a second alert in response to the presence of the match (par. 22).

Regarding claim 14, Currie discloses the method according to claim 13 wherein the first alert is indicative of a specific attack on the first network and the second alert is indicative of a non-specific attack on the first network (par. 44).

Regarding claim 15, Hrabik discloses the method according to claim 12 wherein said step of determining if the characteristic matches a characteristic of an attack upon a second client determines if the characteristic matches a characteristic of attacks upon multiple clients coupled to the multiple client network system (par. 59-61).

Regarding claim 16, Currie discloses the security verification system can maintain and provide security scores and corresponding graphical indicators of individual security attributes, both current and/or historical, of one or more on-line services (par. 23).

Moreover, Hrabik discloses a method of preempting an intrusion comprising the steps of: determining characteristics of an attack upon a first host; and testing a second host for a susceptibility to an attack of the determined characteristics (par. 59-61).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Currie with teachings of Hrabik because it would allow to include an intrusion detector for detecting attacks upon a second computer network as disclosed by Hrabik. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Hrabik to protect a target network from both internal and external intruders (Hrabik, par. 11).

Regarding claim 17, Hrabik discloses the method according to claim 16 further comprising the step of further determining if the characteristic of the attack upon the first host is a new characteristic, wherein said step of testing does not test the susceptibility of the second host if said step of further determining does not determine that the characteristic of the attack upon the first host corresponds to the new characteristic (par. 59).

Regarding claim 18, Hrabik discloses the method according to claim 17 wherein the new characteristic corresponds to a characteristic not previously determined (i.e., an analyzer might determine that a particular event warrants additional scrutiny because a network device on which it was detected is particularly vulnerable to the type of attacks this event is associated with)(par. 59-61).

Regarding claim 19, Hrabik discloses further comprising the step of generating an alert if said step of testing indicates that the second host is susceptible to the determined characteristics (par. 59-61).

Regarding claim 20, Hrabik discloses the method according to claim 16 further comprising the step of filtering the determined characteristics of a plurality of attacks determined by said step of determining and generating an alert signal in response to a substantial increase in frequency or rate of attacks of the characteristic, wherein said step of testing tests the susceptibility of the second host in response to the alert signal (par. 59-60).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Klaes, (U.S. Publication No. 2004/0117658),

Bruton, III et al., (U.S. Patent No. 7,076,803), and

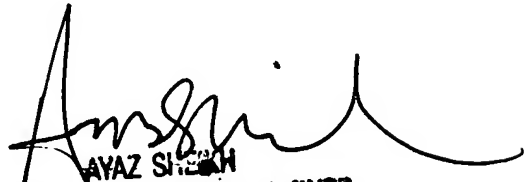
Bunker V. et al., (U.S. Publication No. 2003/0009696).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A.S.
Patent Examiner
Group 2131
March 31, 2007


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100